ROBERT SIBILIA S.B.N. 126979
Oceanside Law Center
P.O. Box 861
Oceanside, CA 92049
Tel: (760) 666-1151
Fax: (818) 698-0300
Email: robert@oceansidelawcenter.com
Attorney for Plaintiff

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

RAMSEY COULTER, individually, and on behalf of all other similarly situated consumers,

Plaintiff,

vs.

DROPBOX, INC.,

Defendant.

Case No.: 3:24-cv-2637

CLASS ACTION COMPLAINT FOR:

1. **NEGLIGENCE**
2. **NEGLIGENCE PER SE**
3. **INVASION OF PRIVACY**
4. **VIOLATION OF THE CALIFORNIA BUSINESS & PROFESSIONS CODE § 17200 *et seq.***

DEMAND FOR JURY TRIAL

Plaintiff, Ramsey Coulter ("Plaintiff"), hereby alleges:

INTRODUCTION

1. With this action, Plaintiff seeks to hold Defendant responsible for the harms it caused Plaintiff in a massive and preventable data breach of Defendant's inadequately protected computer network.

JURISDICTION AND VENUE

2. This Court has original jurisdiction pursuant to 28 U.S.C.§ 1332(d)(2). In the aggregate, Plaintiff's claims, and the claims of the other members of the Class exceed $5,000,000 exclusive of interest and costs, and there are numerous class members who are citizens of states other than Defendant's state of citizenship, which is California.
3. This court has personal jurisdiction over Defendant because Defendant has its headquarters and principal place of business and is authorized to do business in the State of California.
4. Venue is proper in this Court pursuant to 28 U.S.C.§ 1391 because Defendant resides in this District and because Defendant is subject to personal jurisdiction in this District.

PARTIES

5. Plaintiff is a natural person who at all relevant times has resided in Madison, Florida. Plaintiff is a subscriber to, and user of, Defendant's services.
6. Defendant Dropbox, Inc., ("Dropbox" or "Defendant"), is a corporation that has its principal place of business in San Francisco, California.

FACTUAL STATEMENT

7. On April 24th 2024, hackers infiltrated and accessed the inadequately protected computer systems of Defendant and stole the sensitive personal information ("Personal Information" or "PII") of thousands of individuals.
8. The PII taken by the hackers includes: names, addresses, emails, usernames, phone numbers, and hashed passwords, in addition to general account settings and certain

authentication information such as API keys, OAuth tokens, and multi-factor authentication.

9. In short, thanks to Defendant's failure to protect the Breach Victims' Personal Information, cyber criminals were able to steal everything they could possibly need to commit nearly every conceivable form of identity theft and wreak havoc on the financial and personal lives of potentially millions of individuals. This includes logging in to Plaintiff's personal bank accounts, mortgage accounts, and online storage where Plaintiff maintains sensitive personal documents, including medical records, private photographs, and other PII information such as social security number, date of birth, and bank account numbers.

10. Defendant's conduct—failing to implement adequate and reasonable measures to ensure their computer systems were protected, failing to take adequate steps to prevent and stop the breach, failing to timely detect the breach, failing to disclose the material facts that they did not have adequate computer systems and security practices to safeguard the Personal Information, failing to honor their repeated promises and representations to protect the Breach Victims' Personal Information, caused substantial harm and injuries to Plaintiff.

11. As a result of the Data Breach, Plaintiff has suffered damages. First, Plaintiff needed to spend a significant period of time changing several passwords, speaking with his banks, talking with the credit agencies, monitoring his bank accounts, reviewing his credit information, and checking his credit cards. Second, Plaintiff was a recent victim of identity theft, wherein thieves were able to access his bank account to withdraw funds. The likelihood of this occurring repeatedly, as a result of Defendant's data breach, has caused Plaintiff emotional distress, including lack of sleep, worry, anxiety, and stress. Third,

Plaintiff incurred out of pocket costs in paying for communications to third parties in order to alert them to the potential for fraud, and to place freezes on Plaintiff's information.

12. Plaintiff brings this lawsuit to hold Defendant responsible for its negligent and reckless failure to use reasonable, current cybersecurity measures to protect Plaintiff's Personal Information.

13. Because Defendant presented such a soft target to cybercriminals, Plaintiff has already been subjected to violations of their privacy, fraud, and identity theft, or have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff must now and in the future, spend time to more closely monitor credit reports, financial accounts, phone lines, and online accounts to guard against identity theft.

14. Plaintiff seeks actual damages, statutory damages, and punitive damages, with attorney fees, costs, and expenses under negligence, negligence per se, breach of fiduciary duties, breach of confidence, breach of implied contract, and invasion of privacy. Plaintiff also seeks injunctive relief, including significant improvements to Defendant's data security systems, future annual audits, and long-term credit monitoring services funded by Defendant, and other remedies as the Court sees fit.

CLASS ACTION ALLEGATIONS

The Class

15. Plaintiff seeks certification of the class, initially defined as follows:

All consumers that had their data compromised during the 2024 data breach.

16. Excluded from the Class is Defendant herein, and any person, firm, trust, corporation or other entity related to or affiliated with Defendant, including, without limitation, persons who are officers, directors, employees, associates or partners of Defendant.

Numerosity

17. Upon information and belief, Defendants information security system was breached due to flawed policies, impacting many of Defendant's clients. The members of the Class, therefore, are believed to be so numerous that joinder of all members is impracticable.

18. The exact number and identities of the members of the Class are unknown at this time and can only be ascertained through discovery. Identification of the members of the Class is a matter capable of ministerial determination from Defendant's records.

Common Questions of Law and Fact

19. There are questions of law and fact common to the class that predominates over any questions affecting only individual Class members. These common questions of law and fact include, without limitation: (i) whether Defendant failed to adequately protect the information it held in its system; (ii) whether Plaintiff and the Class have been injured by Defendant's conduct; (iii) whether Plaintiff and the Class have sustained damages and are entitled to restitution as a result of Defendant's wrongdoing and, if so, what is the proper measure and appropriate statutory formula to be applied in determining such damages and restitution; and (iv) whether Plaintiff and the Class are entitled to declaratory and/or injunctive relief.

Typicality

20. Plaintiff's claims are typical of the claims of the members of the Class, and Plaintiff has no interests adverse or antagonistic to the interests of other members of the Class.

Protecting the Interests of the Class Members

21. Plaintiff will fairly and adequately represent the Class members' interests in that Plaintiff's counsel is experienced and, further, anticipates no impediments in the pursuit and maintenance of the Class Action as sought herein.

Proceeding Via Class Action is Superior and Advisable

22. A class action is superior to other methods for the fair and efficient adjudication of the claims herein asserted.

23. The members of the Class are generally unsophisticated individuals, whose rights will not be vindicated in the absence of a Class Action.

24. Prosecution of separate actions by individual members of the Class would create the risk of inconsistent or varying adjudications resulting in the establishment of inconsistent or varying standards for the parties.

25. A Class Action will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the duplication of effort and expense that numerous individual actions would engender. Class treatment also will permit the adjudication of relatively small claims by many Class members who could not otherwise afford to seek legal redress for the wrongs complained of herein.

26. Absent a Class Action, the members of the Class will continue to suffer losses borne from Defendant's breaches of Class members' statutorily protected rights as well as monetary damages, thus allowing and enabling: (a) Defendant's conduct to proceed and; (b) Defendant to further enjoy the benefit of its ill-gotten gains.

27. Defendant has acted, and will act, on grounds generally applicable to the entire Class, thereby making appropriate a final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

COUNT I
NEGLIGENCE

28. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.
29. Defendant solicited, gathered, and stored the Personal Information of Plaintiff.
30. Defendant knew, or should have known, of the risks inherent in collecting and storing the Personal Information of Plaintiff and the importance of adequate security.
31. Defendant were well aware of the fact that hackers routinely attempted to access Personal Information without authorization. Defendant also knew about numerous, well publicized data breaches wherein hackers stole the Personal Information from companies who held or stored such information.
32. Defendant owed duties of care to Plaintiff whose Personal Information was entrusted to it. Defendant's duties included the following:
    a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the Personal Information in its possession;
    b. To protect the Personal Information in its possession using reasonable and adequate security procedures and systems;
    c. To adequately and properly train its employees to avoid phishing emails;
    d. To use adequate email security systems, including DMARC enforcement and Sender Policy Framework enforcement, to protect against phishing emails;

e. To adequately and properly train its employees regarding how to properly and securely transmit and store Personal Information;

f. To train its employees not to store Personal Information in their email inboxes longer than absolutely necessary for the specific purpose that it was sent or received;

g. To implement processes to quickly detect a data breach, security incident, or intrusion; and

h. To promptly notify Plaintiff and Class members of any data breach, security incident, or intrusion that affected or may have affected their Personal Information.

33. Because Defendant knew that a security incident, breach or intrusion upon its systems would potentially damage thousands of consumers whose information Defendant held, including Plaintiff, it had a duty to adequately protect their Personal Information.

34. Defendant owed a duty of care not to subject Plaintiff and the Class to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

35. Defendant knew, or should have known, that its security practices and computer systems did not adequately safeguard the Personal Information of Plaintiff.

36. Defendant breached its duties of care by failing to provide fair, reasonable, or adequate computer systems and security practices to safeguard the Personal Information of Plaintiff.

37. Defendant breached its duties of care by failing to provide prompt notice of the Data Breach to the persons whose personal information was compromised.

38. Defendant acted with reckless disregard for the security of the Personal Information of Plaintiff because Defendant knew or should have known that their computer systems and

data security practices were not adequate to safeguard the Personal Information that it collected and stored, which hackers were attempting to access.

39. Defendant acted with reckless disregard for the rights of Plaintiff by failing to provide prompt and adequate notice of the data breach so that they could take measures to protect themselves from damages caused by the fraudulent use of Personal Information compromised in the Data Breach.

40. Defendant also had independent duties under federal and state law requiring them to reasonably safeguard Plaintiff's Personal Information and promptly notify them about the Data Breach.

41. As a direct and proximate result of Defendant's negligent conduct, Plaintiff has suffered damages and remains at imminent risk of further harm.

42. The injury and harm that Plaintiff has suffered (as alleged above) was reasonably foreseeable.

43. The injury and harm that Plaintiff suffered (as alleged above) was the direct and proximate result of Defendant's negligent conduct.

44. Plaintiff has suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
NEGLIGENCE PER SE

45. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

46. Pursuant to the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security to safeguard the Personal Information of Plaintiff.

47. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Personal Information. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

48. Defendant solicited, gathered, and stored the Personal Information of Plaintiff as part of its business of gathering information and presenting itself as a safe cloud storage place for personal information.

49. Defendant violated the FTCA by failing to use reasonable measures to protect the Personal Information of Plaintiff and not complying with applicable industry standards, as described herein.

50. Defendant breached its duties to Plaintiff under the FTCA and other state data security and privacy statutes by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Breach Victim's Personal Information.

51. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

52. Plaintiff are within the class of persons that the FTCA was intended to protect.

53. The harm that occurred as a result of the Data Breach is the type of harm the FTCA, the state data breach privacy statutes were intended to guard against.

54. Defendant breached its duties to Plaintiff under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's Personal Information.

55. Defendant's violation of the FTCA, state data security statutes, and/or the state data breach notification statutes constitute negligence per se.

56. As a direct and proximate result of Defendant's negligence per se, Plaintiff has suffered, and continues to suffer, damages arising from the Data Breach by, inter alia, having to spend time reviewing his bank accounts and credit reports for unauthorized activity; spend time and incur costs to place and re-new a "freeze" on his credit; be inconvenienced by the credit freeze, which requires him to spend extra time unfreezing their account with each credit bureau any time he wants to make use of his own credit; and becoming a victim of identity theft, which may cause damage to their credit and ability to obtain insurance, medical care, and jobs.

57. The injury and harm that Plaintiff suffered was the direct and proximate result of Defendant's negligence per se.

COUNT III
INVASION OF PRIVACY

58. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

59. Plaintiff had a legitimate expectation of privacy regarding the PII and was accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

60. Defendant owed a duty to Plaintiff to keep the PII confidential.

61. Defendant's reckless and negligent failure to protect Plaintiff's PII constitutes an intentional interference with Plaintiff's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

62. In failing to protect Plaintiff's PII, Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

63. Because Defendant failed to properly safeguard Plaintiff's PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff.

64. Defendant knowingly did not notify Plaintiff in a timely fashion about the Data Breach.

65. As a proximate result of Defendant's acts and omissions, Plaintiff's private and sensitive PII was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff to suffer damages.

66. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff since the PII is still maintained by Defendant with their inadequate cybersecurity system and policies.

67. Plaintiff has no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard Plaintiff's PII.

68. Plaintiff, seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's PII.

69. Plaintiff, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT IV
CALIFORNIA BUSINESS AND PROFESSIONS CODE § 17200 *et seq.*

70. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

71. Defendant's conduct constitutes unfair and illegal and fraudulent business practices within the meaning of § 17200.

72. As alleged herein, Defendant's failure to prevent said data breach violates § 17200.

73. Further, Defendant's failure to disclose the data breach for at least a week, allowing third parties a week of unfettered access to Plaintiff's Personal Information constitutes unfair and illegal business practices.

74. Plaintiff, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

75. Said injury stems directly from Defendant's conduct.

WHEREFORE, Plaintiff Ramsey Coulter, respectfully requests that this Court do the following for the benefit of Plaintiff:

A. Enter judgment against Defendant for:

1. Statutory damages;
2. Actual damages;
3. Punitive damages;
4. Litigation costs;
5. and reasonable attorneys' fees.

B. Grant injunctive relief against Defendant to ensure that Defendant adequately maintains the PII that it maintains, and prevent identity theft from that which was already stolen.

Jury Demand

Plaintiff herein demands a trial by jury.

Dated this May 2nd, 2024

Respectfully Submitted,

/s/ Robert Sibilia_____
ROBERT SIBILIA S.B.N. 126979
Oceanside Law Center
P.O. Box 861
Oceanside, CA 92049
Tel: (760) 666-1151
Fax: (818) 698-0300
Email: robert@oceansidelawcenter.com
Attorney for Plaintiff, Ramsey Coulter